UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
CINCINNATI DIVISION

CHARLES NEWMAN, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. TOTAL QUALITY LOGISTICS LLC, Defendant.	Case No.: 20-cv- **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

INTRODUCTION

1. This class action seeks redress for negligence because of the failure of Total Quality Logistics, LLC ("TQL") to implement and maintain reasonable security measures over personally identifiable information.

JURISDICTION AND VENUE

2. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because: (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

3. The Court has personal jurisdiction over Defendant because Defendant's principal offices are located in Cincinnati, Ohio.

4. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District.

PARTIES

5. Plaintiff Charles Newman is a citizen of the State of Wisconsin who resides in Milwaukee County.

6. Plaintiff Newman is the owner and operator of a trucking business. The trucking companies and sole proprietor truck drivers who are members of the putative class in this action are collectively referred to as "carriers."

7. Defendant Total Quality Logistics, LLC ("TQL") is an Ohio limited liability company with its principal offices located at 4289 Ivy Pointe Boulevard, Cincinnati, Ohio 45245.

FACTS

8. Founded in Cincinnati, Ohio in 1997, TQL is a freight brokerage firm, which provides domestic and international freight transportation and logistics services. A freight broker locates motor carriers to pick up and deliver the freight of its customers at specified places and times.

9. TQL's website states that it "connects customers with shipping needs with carriers that have the available capacity and service offerings," and its mission is to "Exceed the customer's expectations at all times and handle their transportation requirements from the moment of pickup until delivery 24/7/365." Indeed, TQL is one of the largest freight brokerage firms in North America, with its website boasting that TQL moved 1.8+ million loads in 2019 and works "with a network of more than 85,000+ carriers to create greater supply chain efficiencies for our customers" and 5,000+ employees across 57 officers in 26 states.

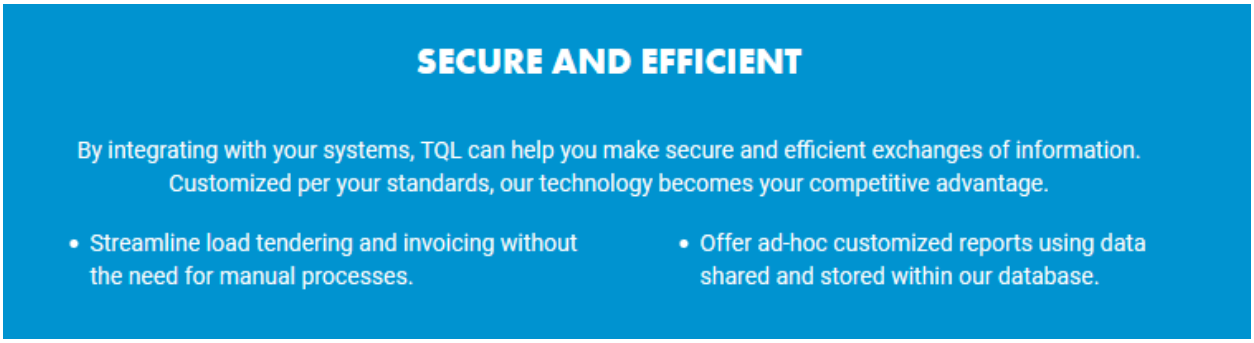
10. Plaintiff Newman and his trucking business do business with TQL. Plaintiff uses TQL's services to find, pickup and deliver freight loads.

11. In the course of providing its brokerage services, TQL has acquired the personal and financial information for many of its carriers — including their social security numbers, tax identification numbers, bank account numbers, and invoice information, including amounts and dates (the "Personal and Financial Information")

12. As a result of TQL's failure to implement and maintain reasonable security measures to protect Personal and Financial Information from unauthorized access, the Personal and Financial Information of Plaintiff and other Class members was accessed and viewed by unauthorized individuals while being maintained on TQL's information and technology servers (the "Data Breach").

13. Upon information and belief, as a result of the Data Breach, Plaintiff's and the other Class members' Personal and Financial Information, and perhaps more information, is now in the hands of unknown persons who intend to use it for criminal or nefarious purposes. Upon information and belief, the unauthorized persons intend to sell the Personal and Financial Information to exploit and injure Plaintiff and the other Class members, to commit identity theft and identity fraud, and commit other acts injurious and detrimental to Plaintiff and the other Class members.

14. Notwithstanding its vulnerabilities, TQL touts the security of its information management systems and protocols. For example, TQL's website's "Data Integration" webpage states:



https://www.tql.com/data-integration.

15. TQL's website also describes its privacy policies with respect to TQL's collection, use, sharing, retention, and security of personal information, business information, and payment and ordering information, which advises that "TQL will not sell or otherwise disclose personal information except as permitted by law, described in this policy, or otherwise disclosed to you," and boasts that while "TQL CANNOT AND DOES NOT GUARANTEE THE SECURITY OR CONFIDENTIALITY OF THE INFORMATION COLLECTED," TQL nonetheless "uses various administrative, technological, and/or physical security measures to protect the information collected." https://www.tql.com/privacy.

16. Plaintiff and the other Class members had their Personal and Financial Information entrusted in the wrong hands. Despite TQL's assurances, it failed to implement and maintain reasonable data security practices in accordance with its representations and the obligations it owes under the law.

17. On February 27, 2018, TQL sent out bulk emails to its carriers and customers, informing them that their information might have been compromised after a recent data breach was discovered in TQL's IT systems on Monday, February 24, 2020.

18. The emails to TQL's customers advised that "email addresses, phone numbers, first and last names and TQL Customer ID numbers" might have been compromised and further

advised that the breach "may have compromised the security of our online portals for a segment of our customers' non-financial data."

19. Internal TQL memos and emails to TQL's carriers advised that the carrier information that was compromised included social security numbers, tax ID numbers, bank account numbers, and invoice information, including invoice amounts and dates.

20. The email to carriers advised them that they could direct "additional questions" to TQL's "carrier response team" by email or phone hotline.

21. The website FreightBrokerLive.com states:

> According to internal sources, the breach was discovered earlier in the week when TQL's accounting department called a carrier to verify changes to their banking information within their system. The carrier reportedly denied knowledge of the change prompting the accounting department to send the issue to the IT department within TQL. Sources say there is evidence the breach occurred ***quite a while before being discovered***, although it is unclear of just how long the hackers were dormant in the system. It appears several carrier's banking information was changed and that payments were sent out to these altered bank accounts. Internal sources say the total amount stolen was less than $100,000. TQL says they have identified less than 20 carriers where ACH payment theft may have occurred.

https://www.freightbrokerlive.com/tql-data-breach-update-what-we-know/ (accessed Feb. 28, 2020).

22. The FreightBrokerLive website further states that the breach was caused by TQL's failure to provide and maintain proper information security protocols:

> Sources tell Fright Broker Live the hackers were able to access the internal IT systems utilizing TQL's mobile applications as a pass through into the system. TQL has since taken steps to close the security gaps in their system, hired an third-party cyber security firm for "additional forensics," on their systems to identify if any other information was compromised. TQL is also working with the Federal Bureau of Investigation and other law enforcement to track the hackers.

https://www.freightbrokerlive.com/tql-data-breach-update-what-we-know/ (accessed Feb. 28, 2020).

23. Contrary to the statement from these "internal sources" that TQL only learned about the Data Breach earlier this week, when Plaintiff dialed the TQL's hotline, he was advised that TQL discovered the data breach within the last few weeks.

24. Upon information and belief, Plaintiff and the other Class members' Personal and Financial Information was accessed, viewed, downloaded, acquired, and stolen by unauthorized persons from TQL's information technology servers.

25. The bulk email is insufficient to comply with TQL's obligations to provide adequate and timely notification of the Data Breach under the law. TQL had already engaged a "third-party cyber security firm" and "taken steps to close the security gaps in their system" when timely notification of the Data Breach was of the essence. Upon information and belief, TQL kept the incident secret from Plaintiff and the other Class members for at least a "few weeks." Indeed, TQL does not even know how long the breach had been ongoing. Data thieves likely had several months from the alleged beginning of the Data Breach until notification to perpetrate fraud using the Personal and Financial Information with no victim aware of the threat, and, in fact, altered banking information and stole payments from a number of carriers.

26. The email did not identify the number of affected individuals. Upon information and belief more than 85,000 carriers were affected.

27. As a direct and foreseeable result of TQL's failures to adopt and maintain adequate security protocols to safeguard its customers' and carriers' Personal and Financial Information, Plaintiff and the other Class members' Personal and Financial Information was placed on unsecure servers. The Personal and Financial Information was accessed, viewed, obtained, downloaded, and is now in the hands of unknown individuals that are undoubtedly intent on using the information to harm Plaintiff and the other Class members.

Data Breaches Lead to Identity Theft

28. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.[1]

29. The Federal Trade Commission ("FTC") cautions that identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[2]

30. Personal and Financial Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[3] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

31. In fact, "[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud."[4]

The Monetary Value of Privacy Protections and Personal Information

---

[1] *See Victims of Identity Theft*, 2014, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 19, 2018).

[2] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[3] Companies, in fact, also recognize personal information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

[4] *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at https://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/ (last visited July 19, 2018).

32. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[5]

33. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[6]

34. The FTC has also recognized that consumer's personal information is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[7]

35. Recognizing the high value that consumers place on their Personal and Financial Information, many companies now offer consumers an opportunity to sell some of this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction

---

[5] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited July 19, 2018).

[6] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited July 19, 2018).

[7] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited July 19, 2018).

transparent, consumers will make a profit from their personal information.[8] This business has created a new market for the sale and purchase of this valuable data.[9]

36. Consumers place a high value not only on their personal information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[10]

FTC Act

37. Additionally, according to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

38. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted

[8] Steve Lohr, *You Want My Personal Data? Reward Me for It, The New York Times*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited July 19, 2018).

[9] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited July 19, 2018).

[10] *See Victims of Identity Theft*, 2014, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 19, 2018).

from the system; and have a response plan ready in the event of a breach.

39. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[11]

40. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Personal Information. These orders provide further guidance to businesses with regard to their data security obligations.

41. As noted above, TQL should have been aware that its security measures were inadequate because hackers could use its mobile applications as a pass-through into its systems.

Damages Sustained by Plaintiff and the Other Class Members

42. Plaintiff and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Personal and Financial Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) the value of their time and expenses associated with mitigation, remediation, and sorting out the risk of fraud and actual instances of fraud; and (v) deprivation of the value of their Personal and Financial Information, for which there is a well-established national and international market.

43. Plaintiff and the other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiff and the other

[11] FEDERAL TRADE COMMISSION, Protecting Personal Information: A Guide for Business (Nov. 2011), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Dec. 20, 2019).

Class members have been forced to expend and must expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

44. Acknowledging the damage to Plaintiff and Class members, TQL is instructing its carriers to "contact your financial institution immediately, letting them know your bank information has been exposed." Plaintiff and the other Class members now face a greater risk of identity theft.

COUNT I – NEGLIGENCE

45. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

46. TQL owed to Plaintiff and the other Class members a duty to exercise reasonable care in handling and using the Personal and Financial Information in its custody, including:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Personal and Financial Information in its possession;

b. to protect Personal and Financial Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices and the practices and certifications represented on its website which it voluntarily undertook duties to implement; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly and sufficiently notifying Plaintiff and the other members of the Class of the Data Breach.

47. TQL knew or should have known the risks of collecting and storing Personal and Financial Information and the importance of maintaining secure systems. TQL knew of the

many breaches that targeted other entities in the years preceding the Data Breach, as illustrated by its own representations alleged herein.

48. Given the nature of TQL's business, the sensitivity and value of the information it maintains, and the resources at its disposal, TQL should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

49. Defendant owed these duties to Plaintiff and the other Class members because Plaintiff and the other Class members are a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited Plaintiff and the other Class members' personal information.

50. Additionally, under Ohio Rev. Code § 1349.19(C) and various other state laws, Defendant owed to Plaintiff and the Class members a duty to notify them within a reasonable timeframe of any breach to the security of their personal information. *See* Digital Guardian, "The Definitive Guide to U.S. State Data Breach Laws" (2018) (available online at: https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf) (accessed: Feb. 28, 2020).

51. TQL breached the duties it owed to Plaintiff and Class members in several ways, including:

a. by failing to implement adequate security systems, protocols and practices sufficient to protect Personal and Financial Information and thereby creating a foreseeable, unreasonable risk of harm;

b. by failing to comply with the minimum industry data security standards and its own assurances of superior data security standards;

c. by negligently performing voluntary undertakings to secure and protect the Personal and Financial Information it solicited and maintained; and

d. by failing to timely and sufficiently discover and disclose to consumers that their Personal and Financial Information had been improperly acquired or accessed, and providing misleading and unfounded suggestions that their information (and by extension their identity) is not in the immediate peril it is in fact in.

e. But for TQL's wrongful and negligent breach of the duties it owed to Plaintiff and the other Class members, their Personal and Financial Information would not have been compromised.

52. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of TQL's negligent conduct. Plaintiff and the other Class members have suffered actual damages including improper disclosure and lost value of their Personal and Financial Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

53. Plaintiff's and the other Class members' injuries were proximately caused by TQL's violations of the common law duties enumerated above, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT II – BREACH OF IMPLIED CONTRACT

54. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

55. In providing Personal Information to TQL, Plaintiff and the other members of the

Class entered into an implied contract with TQL, whereby TQL became obligated to reasonably safeguard Plaintiff's and the other Class members' Personal Information.

56. Under the implied contract, TQL was obligated to not only safeguard Personal Information, but also to provide Plaintiff and the other Class members with prompt, truthful, and adequate notice of any security breach or unauthorized access of said information.

57. TQL breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard Plaintiff's Personal Information.

58. TQL also breached its implied contract with Plaintiff and the other Class members by failing to provide prompt, truthful, and adequate notice of the Data Breach and unauthorized access of their Personal Information by hackers.

59. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) improper disclosure of their Personal Information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (iii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud; (iv) the increased risk of identity theft; and (v) deprivation of the value of their Personal Information, which is likely to be sold to cyber criminals.

COUNT III – NEGLIGENCE *PER SE*

60. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

61. Section 5 of the FTCA prohibits "unfair … practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as TQL, of failing to use reasonable measures to protect payment card data.

62. TQL violated Section 5 of the FTCA by failing to use reasonable measures to protect payment card data and not complying with applicable industry standards, as described herein. TQL' conduct was particularly unreasonable given the nature and amount of payment card data it obtained and stored, and the foreseeable consequences of a data breach at a retail chain as large as TQL, including, specifically, the damages that would result to Plaintiff and Class members.

63. TQL' violation of Section 5 of the FTCA constitutes negligence *per se*.

64. Plaintiff and Class members are within the class of persons that the FTCA was intended to protect.

65. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

66. As a direct and proximate result of TQL' negligence *per se*, Plaintiff and the Class will suffer injuries, including: inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach; false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and forgone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may

take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

CLASS ALLEGATIONS

67. Plaintiff brings this action on behalf of a Class, consisting of:

> All persons residing in the United States of America whose Personal and Financial Information was maintained by TQL during the Data Breach that was disclosed on February 27, 2020, including but not limited to all persons who were sent the February 27, 2020 email informing them of the Data Breach, all persons who were subsequently sent communications informing them of the Data Breach, and all persons whom TQL can identify as having their Personal Information, from February 27, 2020 through the date this class is certified. Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

68. The Class is so numerous that joinder is impracticable. On information and belief, there are more than 85,000 members of the Class.

69. There are questions of law and fact common to the members of the Class, which common questions predominate over any questions that affect only individual members. The predominant common questions include:

a. Whether TQL had a duty to protect Plaintiff and Class members' Personal and Financial Information;

b. Whether TQL knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether TQL security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether TQL was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether TQL's failure to implement adequate data security measures allowed the breach to occur;

f. Whether TQL's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Personal and Financial Information of Plaintiff and Class members;

g. Whether Plaintiff and Class members are entitled to relief.

70. Plaintiff's claims are typical of the claims of the Class members. All are based on the same factual and legal theories.

71. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff has retained counsel experienced in consumer class action cases including data breach litigation.

72. A class action is superior to other alternative methods of adjudicating this dispute. Individual cases are not economically feasible.

JURY DEMAND

73. Plaintiff hereby demands a trial by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant for:

(a) actual damages;

(b) statutory damages;

(c) punitive damages;

(d) injunctive relief;

(e) attorneys' fees, litigation expenses and costs of suit; and

(f) such other or further relief as the Court deems proper.

Dated: February 28, 2020

Respectfully submitted,

/s/ Richard M. Kerger

Richard M. Kerger (0015864)

Richard M. Kerger (0015864)
Kimberly Conklin (0074726)
THE KERGER LAW FIRM, LLC
4159 N. Holland-Sylvania Road, Suite 101
Toledo, OH 43623
Telephone: (419) 255-5990
Fax: (419) 255-5997
Email: rkerger@kergerlaw.com
Kconklin@kergerlaw.com

Shpetim Ademi
John D. Blythin
Mark A. Eldridge
ADEMI & O'REILLY, LLP
3620 East Layton Avenue
Cudahy, WI 53110
(414) 482-8000
(414) 482-8001 (fax)
sademi@ademilaw.com
jblythin@ademilaw.com
meldridge@ademilaw.com